500.41092X00

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re Patent Application of

Mototsugu NISHIOKA

Serial No.: 10/046,224

Filed: January 16, 2002

For: PUBLIC-KEY CRYPTOPGAPHIC SCHEMES SECURE AGAINTS AN ADAPTIVE CHOSEN CIPHERTEXT ATTACK IN THE STANDARD MODEL

Group: 2136

Examiner: D. G. Cervetti

REPLY BRIEF

MS Appeal Briefs - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

September 4, 2007

Sir:

This Reply Brief is respectfully submitted in response to the Examiner's Answer mailed July 3, 2007, and does not include any new or non-admitted amendment, or any new or non-admitted affidavit or other evidence, in compliance with 37 C.F.R. 41.41. Entry and consideration of this Reply Brief are requested.

I. REAL PARTY IN INTEREST

The statement of the Real Party in Interest contained in the Appeal Brief is correct, as the Examiner affirmed in the Examiner's Answer.

Accordingly, the Real Party in Interest in this Appeal is Hitachi, Ltd., as evidenced by the Assignment filed on February 26, 2002 in Application Serial No. 10/046,224, filed January 16, 2002, said application being the subject of this Appeal, and recorded on Reel 012624 and Frame 0156.

II. RELATED APPEALS AND INTERFERENCES

The statement of the Related Appeals and Interferences contained in the Appeal Brief is correct, as the Examiner affirmed in the Examiner's Answer.

Accordingly, there are no other Appeals or Interferences that may directly affect, may be directly affected by, or have a bearing on the Board's decision in this appeal.

III. STATUS OF CLAIMS

The statement of the status of the claims in the Appeal Brief is incorrect, as the Examiner affirmed in the Examiner's Answer. The statement of the status of the claims in the Examiner's Answer is correct. Accordingly, the status of the claims is as follows:

Claims 23-44 are currently pending.

Claims 23-44 are being appealed.

Claims 23-44 are rejected under 35 USC §112, second paragraph as being indefinite for failing to particularly point out and distinctly claim the subject matter which Appellants regard as their invention; and

Claims 23-44 are rejected under 35 U.S.C. §103(a) as being unpatentable over U. S. Patent No. 6,697,488 to Cramer et al. ("Cramer").

Accordingly, claims 23-44 constitute the claims on appeal, and all stand rejected in the final Office Action of February 7, 2006. A copy of claims 23-44 is attached as pages 57-72 of the Appeal Brief.

IV. STATUS OF AMENDMENTS

The statement of the status of the Amendments after Final rejection contained in the Examiner's Answer is correct, with the exception that the Examiner did not address the Amendment after Final filed on February 7, 2007.

As indicated by the Examiner in the Examiner's Answer, the Amendment filed September 7, 2006 has been entered, and as indicated by the Amendment after Final initialed by the Examiner on April 18, 2007, the Amendment filed February 7, 2007 has been entered.

Accordingly, the Appendix being submitted with the present Reply Brief incorporates the amendments to claims 23-44, which were filed on February 7, 2007. No other amendments were filed after final rejection.

V. SUMMARY OF THE CLAIMED SUBJECT MATTER

The statement of the summary of the claimed subject matter contained in the Appeal Brief is correct, as the Examiner affirmed in the Examiner's

Answer.

Accordingly, the summary of the invention is included on pages 3-15 of the Appeal Brief.

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

The statement of the grounds of rejection to be reviewed on appeal contained in the Appeal Brief is incorrect, as the Examiner affirmed in the Examiner's Answer. The statement of the grounds for rejection to be reviewed on appeal contained in the Examiner's Answer is correct.

Accordingly, the statement of the grounds of rejection to be reviewed on appeal is as follows:

Whether claims 23-44 are indefinite under 35 USC §112, second paragraph; and

Whether claims 23-44 are obvious over Cramer under 35 USC §103(a).

VII. ARGUMENT

Appellants make the following response to the various arguments made by the Examiner.

A. 35 USC §112, second paragraph rejection of claims 23-44

As a preliminary matter, the Examiner indicates on page 2 of the Examiner's Answer, under the Status of Claims heading, that claims 23-44 are rejected under 35 U.S.C. §112, second paragraph. However, on page 4-5 of the Examiner's Answer, the Examiner only provides specific rejections for

claims 23, 24, 28, 30, 35, 36, 40, and 41 (the independent claims). Furthermore, on page 24 of the Examiner's Answer, under the Response to Argument heading, the Examiner refers to the rejection of claims 25-27, 29, 31-34, 37-39, and 42-44. Therefore, it appears that the Examiner intended to indicate that the remaining claims 25-27, 29, 31-34, 37-39, and 42-44 inherit the deficiencies of their respective independent claims.

With regard to the rejection of claims 23-44, the Examiner indicates on page 25 that "A clear definition of the variables would overcome this 112 rejection", and further indicates that "Similar argument applies to the remaining independent claims."

In response to the Examiner, Appellants submit that the elements referred to by the Examiner are well known to one of ordinary skill in the art, and do not require any further definition. Nonetheless, Appellants respectfully invite the Board to provide a statement of how to overcome this rejection.

i. Claims 23, 28, 35, and 40

Claims 23, 28, 35, and 40 are rejected as failing to provide sufficient antecedent basis for "$\alpha_1 \,||\, \alpha_2 < q$". In the Response to Argument section on page 24-25 of the Examiner's Answer, the Examiner indicates that Appellants failed to address the insufficient antecedent basis issues raised in the previous office action.

In response to the Examiner, Appellants submit that this rejection is traversed. With regard to claim 23, for example, Appellants submit that the first recitation of $\alpha_1 \,||\, \alpha_2 < q$ appears in line 14, and is not preceded by "the".

Accordingly, there is sufficient antecedent basis for this limitation. Similar arguments apply for the remaining claims 28, 35 and 40.

Furthermore, Appellants submit that the elements of $\alpha_1 || \alpha_2 < q$ are well known to one of ordinary skill in the art, and do not require any further definition. However, Appellants respectfully invite the Board to provide a statement of how to overcome this rejection.

ii. Claims 24, 40 and 41

Claims 24, 40 and 41 are rejected as failing to provide sufficient antecedent basis for "ciphertext and by using the secret key, α'_1, α'_2, m'". In the Response to Argument section on page 24-25 of the Examiner's Answer, the Examiner indicates that Appellants failed to address the insufficient antecedent basis issues raised in the previous office action.

In response to the Examiner, Appellants submit that this rejection is traversed. Appellants submit that the Examiner is improperly combining individual features of claims 24, 40 and 41 to make a single feature. However, the "ciphertext", the "secret key" and "α'_1, α'_2, m'" should be treated separately.

With regard to claim 24, for example, Appellants submit that the first recitation "ciphertext" occurs in line 16 (i.e., "transmitting (u_1, u_2, e, v) as a ciphertext"). Similar arguments apply to claims 40 and 41.

With further regard to claim 24, for example, Appellants submit that the first recitation of "a secret key" occurs in line 3. Accordingly, there is sufficient antecedent basis for this limitation. Similar arguments apply to claims 40 and 41.

With even further regard to claim 24, for example, Appellants submit that the first recitation of "α'_1, α'_2, m'" occurs in line 18, and is not preceded by "the". Accordingly, there is sufficient antecedent basis for this limitation. Similar arguments apply to claims 40 and 41.

Furthermore, Appellants submit that the elements of α'_1, α'_2, m' are well known to one of ordinary skill in the art, and do not require any further definition. However, Appellants respectfully invite the Board to provide a statement of how to overcome this rejection.

iii. Claim 30

Claim 30 is rejected as failing to provide proper antecedent basis for the following limitation:

$$m = D_{K'}(C)$$

In the Response to Argument section on pages 24-25 of the Examiner's Answer, the Examiner indicates that Appellants failed to address the insufficient antecedent basis issues raised in the previous office action.

In response to the Examiner, Appellants submit that this rejection is traversed. Appellants submit that the first recitation of this limitation occurs in line 29, and is not preceded by "the". Accordingly, there is sufficient antecedent basis for this limitation.

Furthermore, Appellants submit that the elements of the above-identified limitation are well known to one of ordinary skill in the art, and do not require any further definition. However, Appellants respectfully invite the Board to provide a statement of how to overcome this rejection.

iv. Claim 36

Claim 36 is rejected as failing to provide proper antecedent basis for "transmitting the ciphertext (u_1, u_2, v, C)". In the Response to Argument section on page 24-25 of the Examiner's Answer, the Examiner indicates that Appellants failed to address the insufficient antecedent basis issues raised in the previous office action.

In response to the Examiner, Appellants submit that this rejection is traversed. Appellants submit that the first recitation of this limitation occurs in line 16, and is not preceded by "the". Accordingly, there is sufficient antecedent basis for this limitation.

Furthermore, Appellants submit that the elements of the above-identified limitation are well known to one of ordinary skill in the art, and do not require any further definition. However, Appellants respectfully invite the Board to provide a statement of how to overcome this rejection.

v. Claims 28, 40 and 41

Claims 28, 40 and 41 are rejected as failing to provide proper antecedent basis for the following limitation:

"$. . . = D_{sk}(e)$"

In the Response to Argument section on page 24-25 of the Examiner's Answer, the Examiner indicates that Appellants failed to address the insufficient antecedent basis issues raised in the previous office action.

In response to the Examiner, Appellants submit that this rejection is traversed. Regarding claim 28, Appellants submit that the above-identified limitation is not recited in claim 28. With regard to claims 40 and 41, Appellants submit that the first recitation of this limitation occurs in lines 28 and 22, respectively, and is not preceded by "the". Accordingly, there is sufficient antecedent basis for this limitation.

Furthermore, Appellants submit that the elements of the above-identified limitation are well known to one of ordinary skill in the art, and do not require any further definition. However, Appellants respectfully invite the Board to provide a statement of how to overcome this rejection.

Accordingly, Appellants submit that each of claims 23-44 are definite and fully comply with the requirements of 35 USC §112, second paragraph. Therefore, reconsideration and withdrawal of the 35 USC §112, second paragraph rejection of claims 23-44 are respectfully requested.

B. 35 USC §103(a) rejection of claims 23-44

i. Independent Claim 23

One feature of the present invention, as recited in independent claim 23, includes a key generation step of generating a secret key and a public key. The secret key includes x_1, x_2, y_{11}, y_{12}, y_{21}, y_{22}, and z. The public key includes elements d_1 and d_2. The element d_1 relates to the elements y_{11} and y_{12} of the secret key, and the element d_2 relates to the elements y_{21} and y_{22} of the secret key. Cramer does not disclose this feature.

In response to Appellants' arguments that Cramer does not teach or suggest where the public key includes elements d_1 and d_2, the Examiner asserts on page 26 of the Examiner's Answer that Cramer teaches "d_i" (citing section V, column 9), and thus "d_i" can change and varies.

In response to the Examiner's arguments, Appellants note that in column 9, lines 57-58, Cramer discloses where the group element d is changed by $d_1, \ldots, d_k$, where $1 \leq i \leq k$. However, Cramer is silent as to the value of k used to implement the Cramer system. The present invention uses elements d_1 and d_2, which corresponds to k=2, and Appellants submit that in actual implementation of Cramer, k is larger than or equal to 4.

With regard to the actual implementation of Cramer, Appellants submit that although Cramer is silent as to the value of k used to implement the Cramer system, the article *A Practical Public Key Cryptosystem Provably Secure against Adaptive Chosen Ciphertext Attack*, by Cramer, et al. ("Cramer Article") provides the value of k used to implement the Cramer system. The Cramer Article was submitted in an Information Disclosure Statement (IDS) on February 7, 2007, and was considered by the Examiner on April 20, 2007.

As described on page 15 under section 5.3, the Cramer Article discusses a hypothetical situation where if strings needed to hash in an original scheme are of the form $(a_1, \ldots, a_k)$, where $0 \leq a_i \leq p$. The input to the hash function is u_1, u_2, e € G, and is expressed by the bit series $u_1 \| u_2 \| e$ (where $\|$ means concatenation). When the bit series is expressed using a_i,

where $0 \leq a_i \leq q$, it can be expressed as $a_1 \| \ldots \| a_k$. The minimum k is selected.

With further reference to the Cramer Article, regarding security, the prime number p should have at least 1024 bits in the multiplicative group. If p has 1024 bits, the prime number q becomes maximum when q satisfies $p - 1 = 2q$, and q has 1023 bits. u_1, u_2 and e have 1024 bits, respectively. When $u_1 \| u_2 \| e$ is expressed using concatenation of a_i, which has less than or equal to 1023 bits, the concatenation number k will be at least 4.

When $u_i = g_i^r$ (i = 1, 2) is calculated for the encryption, r has 1023 bits and the exponent number is large. Accordingly, the efficiency of the calculation is poor. In the Cramer Article, when the hash function is not used, v is calculated using the expression on page 15 (sixth line from the bottom). If q is a small number, k becomes large, and the calculation amount of v also becomes large.

In response to Appellants' arguments that in the present invention, k is kept small, the Examiner asserts on page 26 of the Examiner's Answer that features upon which Appellants rely upon (i.e., k is 2 and kept small) are not recited in the rejected claims.

In response to the Examiner's arguments, and as previously discussed, the present invention uses elements d_1 and d_2, which corresponds to k=2. The correspondence between d and k is well known to one of ordinary skill in the art. Therefore, it is not necessary to include k in the claims.

In response to Appellants' arguments that Cramer does not teach or suggest where the secret key includes y_{11}, y_{12}, y_{21}, y_{22}, the Examiner asserts on page 26 of the Examiner's Answer that Cramer expressly claims "choosing at least a first, second, and third . . ." (citing claim 1).

In response the Examiner's arguments, Appellants direct the Examiner's attention to the context and entirety of the language used in claim 1 of Cramer. The claim language of Cramer recites "choosing at least a first, second, and third exponent-number (x_1, x_2, z) as part of a private key." As described in column 7, lines 11-19, Cramer discloses where a first exponent-number x_1, a second exponent-number x_2, a third exponent-number z, a fourth exponent-number y_1, and a fifth exponent-number y_2, are chosen at random for the private key. As such, Cramer discloses the use of elements y_1 and y_2, and the "choosing at least a first, second, and third" language referred to in claim 1 of Cramer does not refer to "choosing at least a first, second, and third" of elements y_1 and y_2. Unlike Cramer, in the present invention, the secret key includes y_{11}, y_{12}, y_{21}, y_{22}. Cramer does not teach or suggest the additional elements of the claimed invention, and the claim language of Cramer cited by the Examiner does not refer to the additional elements in the group y_{11}, y_{12}, y_{21}, y_{22} of the present invention.

Furthermore, as described in column 9, lines 65-67, Cramer describes where, in order to achieve security against lunch-time attacks, "one can simplify the above-described basic scheme" by omitting d, y_1 and y_2. As such, Cramer teaches away from adding additional elements, so as to include both elements d_1 and d_2 in the public key, and each of elements y_{11}, y_{12}, y_{21}, y_{22} in the secret key. Therefore, contrary to the Examiner's assertions, it would not

be obvious to modify Cramer to add the additional elements, so as to achieve the present invention.

In response to Appellants' arguments that Cramer teaches away from adding additional elements to obtain the present invention (i.e., y_{11}, y_{12}, y_{21}, y_{22}), the Examiner asserts on pages 29-30 (with reference to the rejection of claim 30) that Cramer suggests the use of more elements (citing claims 1, 11 and 20). Specifically, the Examiner asserts that the language "choosing at least" implies that more elements may be added.

In response to the Examiner's arguments, Appellants direct the Examiner's attention to the specific language in claims 1, 11 and 20 that follows "choosing at least". There is no disclosure in claims 1, 11 or 20 of choosing at least elements including the element y. The "choosing at least" phrase precedes x_1, x_2, Z, g_1, g_2, etc., but does not precede the element y. Therefore, contrary to the Examiner's assertions, Cramer does teach away from adding the additional elements to obtain y_{11}, y_{12}, y_{21}, y_{22}, as in the present invention.

Therefore, Cramer fails to teach or suggest "a key generation step of generating a secret-key:

- $x_1, x_2, y_{11}, y_{12}, y_{21}, y_{22}, z \in \mathbb{Z}_q$

and a public-key:

- G, G' : finite (multiplicative) group $G \subseteq G'$
- q : prime number (the order of G)
- $g_1, g_2 \in G$
- $c = g_1^{x_1} g_2^{x_2}$, $d_1 = g_1^{y_{11}} g_2^{y_{12}}$, $d_2 = g_1^{y_{21}} g_2^{y_{22}}$, $h = g_1^{z}$,
- $\pi : X_1 \times X_2 \times M \longrightarrow G'$: one-to-one mapping
- $\pi^{-1} : \mathrm{Im}(\pi) \longrightarrow X_1 \times X_2 \times M$

where the group G is a partial group of the group G', X_1 and X_2 are an infinite set of positive integers which satisfy:

$$\alpha_1 || \alpha_2 < q \qquad (\forall \alpha_1 \in X_1, \forall \alpha_2 \in X_2)$$

where M is a plaintext space" as recited in independent claim 23.

Another feature of the present invention, as recited in independent claim 23, includes a ciphertext generation and transmission step of selecting random numbers for a plaintext m, calculating u_1, u_2, e, and v, where:

$$e = \pi(\alpha_1, \alpha_2, m)\, h_r \text{ , and } v = g_1^{\alpha 1}\, c^r\, d_1^{\alpha r}\, d_2^{mr} \text{ .}$$

Cramer does not disclose this feature.

In response to Appellants' arguments that Cramer fails to teach or suggest $e = \pi(\alpha_1, \alpha_2, m)\, h_r$ and $v = g_1^{\alpha 1}\, c^r\, d_1^{\alpha r}\, d_2^{mr}$, the Examiner asserts on page 27 of the Examiner's Answer that Cramer expressly teaches performing calculations with the specific elements to obtain keys and decrypted data (citing claims 1 and 11; and column 11, lines 43-60). The Examiner further asserts that adding, subtracting, raising to the power, or performing a mod operation without clearly defining what the numbers are do not patentably distinguish the present invention over the Cramer reference.

In response to the Examiner's arguments, Appellants submit that the elements contained in the claims are well known to one of ordinary skill in the art. Therefore, further defining the elements is not necessary. Furthermore, whether or not the terms are clearly defined, Cramer still fails to teach the

features of the present invention, and is clearly different from the claimed invention.

For example, the verification cipher-number v, as calculated in Cramer (i.e., $v = c^r d^{r\alpha}$) is quite different from v, as calculated in the present invention (i.e., $v = g_1^{\alpha 1} c^r d_1^{\alpha r} d_2^{mr}$), and the Examiner has not provided any explanation as to why one of ordinary skill in the art would be motivated to modify Cramer to obtain this feature. In the present invention, the calculation of v is improved and k can be a small number. This is quite different from Cramer, where as described in the Cramer Article, k is equal to or greater than 4. In the present invention, r can be set small, and the encryption calculation can be efficiently performed.

By way of further example, as shown in column 8, line 5, Cramer discloses where the encryption cipher-number e is calculated according to the following formula: $e = h^r m$. This is quite different from the present invention, where $e = \pi(\alpha_1, \alpha_2, m) h_r$, and the Examiner has not provided any explanation as to why one of ordinary skill in the art would be motivated to modify Cramer to obtain this feature.

Therefore, Cramer fails to teach or suggest "a ciphertext generation and transmission step of selecting random numbers $\alpha_1 \in X_1$, $\alpha_2 \in X_2$, $r \in Z_q$ for a plaintext m ($m \in M$), calculating:

$$u_1 = g_1^r, \quad u_2 = g_2^r, \quad e = \pi(\alpha_1, \alpha_2, m) h^r, \quad v = g_1^{\alpha_1} c^r d_1^{\alpha r} d_2^{mr}$$

where $\alpha = \alpha_1 \| \alpha_2$, and transmitting ($u_1$, u_2, e, v) as a ciphertext" as recited in independent claim 23.

Yet another feature of the present invention, as recited in independent claim 23, includes a ciphertext reception and decipher step. This step includes a condition, such that a step is performed of outputting m' as the deciphered results, if the following is satisfied:

$$g_1{}^{\alpha'_1} u_1{}^{x_1+\alpha' y_{11}+m' y_{21}} u_2{}^{x_2+\alpha' y_{12}+m' y_{22}} = v$$

If the above condition is not satisfied, then a step is performed of outputting as the decipher results the effect that the received ciphertext is rejected. Cramer does not disclose this feature.

In response to Appellants' arguments that Cramer fails to teach or suggest the above-identified condition, the Examiner asserts on page 27 of the Examiner's Answer that Cramer expressly teaches performing calculations with the specific elements to obtain keys and decrypted data (citing claims 1 and 11; and column 11, lines 43-60). The Examiner further asserts that adding, subtracting, raising to the power, or performing a mod operation without clearly defining what the numbers are do not patentably distinguish the present invention over the Cramer reference.

In response to the Examiner's arguments, Appellants submit that the elements contained in the claims are well known to one of ordinary skill in the art. Therefore, further defining the elements is not necessary. Furthermore, whether or not the terms are clearly defined, Cramer still fails to teach the features of the present invention, and is clearly different from the claimed invention.

For example, as described in column 8, lines 50-62, Cramer discloses a condition [1]: $u_1^{x1+y1a}\ u^{x2+y2a} = v$. The condition [1] of Cramer is not the same as the above-described condition of the present invention. Accordingly, Cramer does not disclose the claimed feature, and the Examiner has not provided any explanation as to why one of ordinary skill in the art would be motivated to modify Cramer to obtain this feature.

Therefore, Cramer fails to teach or suggest "a ciphertext reception and decipher step of calculating from the received ciphertext and by using the secret key, α'_1, α'_2, m' ($\alpha'_1 \epsilon X_1$, $\alpha'_2 \epsilon X_2$, $m' \epsilon M$) which satisfy:

$$\pi(\alpha'_1, \alpha'_2, m') = e/u_1{}^z$$

and if the following is satisfied:

$$g_1{}^{\alpha'_1} u_1{}^{x_1+\alpha' y_{11}+m' y_{21}} u_2{}^{x_2+\alpha' y_{12}+m' y_{22}} = v$$

outputting m' as the deciphered results (where $\alpha' = \alpha'_1 \| \alpha'_2$), whereas if not satisfied, outputting as the decipher results the effect that the received ciphertext is rejected" as recited in independent claim 23.

ii. Independent Claim 24

One feature of the present invention, as recited in independent claim 24, includes a key generation step of generating a secret key and a public key. The secret key includes x_1, x_2, y_{11}, y_{12}, y_{21}, y_{22}, and z. The public key includes elements d_1 and d_2, and the elements c, d_1, d_2, and h are calculated using modulo arithmetic. The element d_1 relates to the elements y_{11} and y_{12}

of the secret key, and the element d_2 relates to the elements y_{21} and y_{22} of the secret key. Cramer does not disclose this feature.

In response to Appellants' arguments that Cramer does not teach or suggest where the public key includes elements d_1 and d_2, the Examiner asserts on page 26 of the Examiner's Answer that Cramer teaches "d_i" (citing section V, column 9), and thus "d_i" can change and varies.

In response to the Examiner's arguments, Appellants note that in column 9, lines 57-58, Cramer discloses where the group element d is changed by $d_1, \ldots, d_k$, where $1 \leq i \leq k$. However, Cramer is silent as to the value of k used to implement the Cramer system. The present invention uses elements d_1 and d_2, which corresponds to k=2, and as previously discussed with reference to the Cramer Article, Appellants submit that in the actual implementation of Cramer, k is larger than or equal to 4.

In response to Appellants' arguments that Cramer does not teach or suggest where the secret key includes y_{11}, y_{12}, y_{21}, y_{22}, the Examiner asserts on page 27 of the Examiner's Answer that Cramer expressly claims "choosing at least a first, second, and third . . ." (citing claim 1).

In response the Examiner's arguments, Appellants direct the Examiner's attention to the context and entirety of the language used in claim 1 of Cramer. The claim language of Cramer recites "choosing at least a first, second, and third exponent-number (x_1, x_2, z) as part of a private key." As described in column 7, lines 11-19, Cramer discloses where a first exponent-number x_1, a second exponent-number x_2, a third exponent-number z, a fourth

exponent-number y_1, and a fifth exponent-number y_2, are chosen at random for the private key. As such, Cramer discloses the use of elements y_1 and y_2, and the "choosing at least a first, second, and third" language referred to in claim 1 of Cramer does not refer to "choosing at least a first, second, and third" of elements y_1 and y_2. Unlike Cramer, in the present invention, the secret key includes y_{11}, y_{12}, y_{21}, y_{22}. Cramer does not teach or suggest the additional elements of the claimed invention, and the claim language of Cramer cited by the Examiner does not refer to the additional elements in the group y_{11}, y_{12}, y_{21}, y_{22} of the present invention.

Furthermore, as previously discussed, Cramer teaches away from adding additional elements to obtain the present invention. As described in column 9, lines 65-67, Cramer describes where, in order to achieve security against lunch-time attacks, "one can simplify the above-described basic scheme" by omitting d, y_1 and y_2. As such, Cramer teaches away from adding additional elements, so as to include both elements d_1 and d_2 in the public key, and each of elements y_{11}, y_{12}, y_{21}, y_{22} in the secret key. Therefore, contrary to the Examiner's assertions, it would not be obvious to modify Cramer to add the additional elements, so as to achieve the present invention.

In response to Appellants' argument that Cramer teaches away from adding additional elements to obtain the present invention (i.e., y_{11}, y_{12}, y_{21}, y_{22}), the Examiner asserts on pages 29-30 (with reference to the rejection of claim 30) that Cramer suggests the use of more elements (citing claims 1, 11 and 20). Specifically, the Examiner asserts that the language "choosing at least" implies that more elements may be added.

In response to the Examiner's arguments, Appellants direct the Examiner's attention to the specific language in claims 1, 11 and 20 that follows "choosing at least". There is no disclosure in claims 1, 11 or 20 of choosing at least elements including the element y. The "choosing at least" phrase precedes x_1, x_2, Z, g_1, g_2, etc., but does not precede the element y. Therefore, contrary to the Examiner's assertions, Cramer does teach away from adding the additional elements to obtain y_{11}, y_{12}, y_{21}, y_{22}, as in the present invention.

In response to Appellants' arguments that Cramer does not teach or suggest the use of modulo arithmetic in the equations used to calculate c, d_1, d_2, and h, the Examiner does not provide any arguments for claim 24. However, as best can be determined, with reference to the Examiner's response regarding claim 23 on page 27 of the Examiner's Answer, it appears that the Examiner's position is that Cramer expressly teaches performing calculations with the specific elements to obtain keys and decrypted data (citing claims 1 and 11; and column 11, lines 43-60). Specifically, the Examiner asserts that adding, subtracting, raising to the power, or performing a mod operation without clearly defining what the numbers are do not patentably distinguish the present invention over the Cramer reference.

In response to the Examiner's arguments, Appellants submit that the elements contained in the claims are well known to one of ordinary skill in the art. Therefore, further defining the elements is not necessary. Furthermore, whether or not the terms are clearly defined, Cramer still fails to teach the

features of the present invention, and is clearly different from the claimed invention.

For example, column 7, lines 25-27 of Cramer describes where the public key is "represented by the numbers g_1, g_2, c, d, and h", and column 7, line 25 shows the calculations used to derive the numbers c, d and h. As shown, Cramer does not disclose the use of modulo arithmetic in the equations used to calculate c, d and h. This is quite different from the present invention, where the step of generating a public key includes the elements c, d_1, d_2, and h, which are calculated using modulo arithmetic. Accordingly, Cramer does not teach generating a public key in the manner claimed, and the Examiner has not provided any explanation as to why one of ordinary skill in the art would be motivated to modify Cramer to obtain this feature.

Therefore, Cramer fails to teach or suggest "a key generation step of generating a secret-key:

- $x_1, x_2, y_{11}, y_{12}, y_{21}, y_{22}, z \in \mathbb{Z}_q$

and a public-key:

- p, q : prime number (q is a prime factor of p-1)
- $g_1, g_2 \in \mathbb{Z}_p$: $\mathrm{ord}_p(g_1) = \mathrm{ord}_p(g_2) = q$
- $c = g_1^{x_1} g_2^{x_2} \bmod p$, $d_1 = g_1^{y_{11}} g_2^{y_{12}} \bmod p$, $d_2 = g_1^{y_{21}} g_2^{y_{22}} \bmod p$, $h = g_1^{z} \bmod p$,
- k_1, k_2, k_3 : positive constant $(10^{k_1+k_2} < q,\ 10^{k_3} < q,\ 10^{k_1+k_2+k_3} < p)$

" as recited in independent claim 24.

Another feature of the present invention, as recited in independent claim 24, includes a ciphertext generation and transmission step of selecting random numbers for a plaintext m, calculating u_1, u_2, e, and v, where:

$$u_1 = g_1^{r} \bmod p, \quad u_2 = g_2^{r} \bmod p, \quad e = \tilde{m}\, h^{r} \bmod p, \quad v = g_1^{\alpha_1} c^{r} d_1^{\alpha r} d_2^{mr} \bmod p$$

Cramer does not disclose this feature.

In response to Appellants' arguments that the present invention distinguishes over Cramer because unlike Cramer, the present invention does not rely upon a hash function, and thus, does not use a hash-value a, as in Cramer, the Examiner asserts on page 25 of the Examiner's Answer that Cramer teaches that the use of a hash function can be omitted (citing column 9, lines 60-67).

In response to the Examiner's arguments, Appellants acknowledge that Cramer teaches where the hash function can be omitted. However, the present invention is different from Cramer in the feature used instead of the hash function. The calculation of v is unique to the present invention. Specifically, the verification cipher-number v, as calculated in Cramer (i.e., $v = c^{r} d^{a}$) and which uses the hash value a, is quite different from v, as calculated in the present invention (i.e., $v = g_1^{\alpha 1} c^{r} d_1^{\alpha r} d_2^{mr} \bmod p$), and the Examiner has not provided any explanation as to why one of ordinary skill in the art would be motivated to modify Cramer to obtain this feature. Furthermore, even if Cramer omits the hash function from the equation, Cramer still does not teach the unique calculation of v, as in the present invention.

In response to Appellants' arguments that Cramer does not disclose the use of modulo arithmetic in the equations used to calculate u_1, u_2, e, and v, the Examiner does not provide any arguments for claim 24. However, as best can be determined, with reference to the Examiner's response regarding claim 23 on page 27 of the Examiner's Answer, it appears that the Examiner's position is that Cramer expressly teaches performing calculations with the specific elements to obtain keys and decrypted data (citing claims 1 and 11; and column 11, lines 43-60). Specifically, the Examiner asserts that adding, subtracting, raising to the power, or performing a mod operation without clearly defining what the numbers are do not patentably distinguish the present invention over the Cramer reference.

In response to the Examiner's arguments, Appellants submit that the elements contained in the claims are well known to one of ordinary skill in the art. Therefore, further defining the elements is not necessary. Furthermore, whether or not the terms are clearly defined, Cramer still fails to teach the features of the present invention, and is clearly different from the claimed invention. Specifically, Cramer is quite different from the present invention, where the step of generating a public key includes where the elements u_1, u_2, e, and v are calculated using modulo arithmetic. Accordingly, Cramer does not teach generating a public key in the manner claimed, and the Examiner has not provided any explanation as to why one of ordinary skill in the art would be motivated to modify Cramer to obtain this feature.

Therefore, Cramer fails to teach or suggest "a ciphertext generation and transmission step of selecting random numbers $a = a_1 || a_2$ ($|a_1| = k_1$, $|a_2|$

$= k_2$) for a plaintext m ($|m| = k_3$ where $|x|$ is the number of digits of x), calculating:

$$\tilde{m} = \alpha || K$$

selecting a random number $r \epsilon Z_q$, calculating:

$$u_1 = g_1^r \bmod p, \quad u_2 = g_2^r \bmod p, \quad e = \tilde{m}\, h^r \bmod p, \quad v = g_1^{\alpha_1} c^r d_1^{\alpha r} d_2^{mr} \bmod p$$

and transmitting (u_1, u_2, e, v) as a ciphertext" as recited in independent claim 24.

Yet another feature of the present invention, as recited in independent claim 24, includes a ciphertext reception and decipher step. This step includes a condition, such that a step is performed of outputting m' as the deciphered results, if the following is satisfied:

$$g_1^{\alpha'_1} u_1^{x_1+\alpha' y_{11}+m' y_{21}} u_2^{x_2+\alpha' y_{12}+m' y_{22}} \equiv v \pmod p$$

If the above condition is not satisfied, then a step is performed of outputting, as the decipher results, the effect that the received ciphertext is rejected. Cramer does not disclose this feature.

In response to Appellants arguments that Cramer fails to teach or suggest the above-identified condition, the Examiner does not provide any arguments for claim 24. However, as best can be determined, with reference to the Examiner's response regarding claim 23 on page 27 of the Examiner's Answer, it appears that the Examiner's position is that Cramer expressly

teaches performing calculations with the specific elements to obtain keys and decrypted data (citing claims 1 and 11; and column 11, lines 43-60). The Examiner further asserts that adding, subtracting, raising to the power, or performing a mod operation without clearly defining what the numbers are do not patentably distinguish the present invention over the Cramer reference.

In response to the Examiner's arguments, Appellants submit that the elements contained in the claims are well known to one of ordinary skill in the art. Therefore, further defining the elements is not necessary. Furthermore, whether or not the terms are clearly defined, Cramer still fails to teach the features of the present invention, and is clearly different from the claimed invention.

For example, as described in column 8, lines 50-62, Cramer discloses a condition [1]: $u_1^{x1+y1a}\ u^{x2+y2a} = v$. The condition [1] of Cramer is not the same as the above-described condition of the present invention. Accordingly, Cramer does not disclose the claimed feature, and the Examiner has not provided any explanation as to why one of ordinary skill in the art would be motivated to modify Cramer to obtain this feature.

Therefore, Cramer fails to teach or suggest "a ciphertext reception and decipher step of calculating from the received ciphertext and by using the secret key, α'_1, α'_2, m' ($|\alpha'_1| = k_1$, $|\alpha'_2| = k_2$, $|m'| = k_3$) which satisfy:

$$\alpha'_1||\alpha'_2||m' = e/{u_1}^z \bmod p$$

and if the following is satisfied:

$${g_1}^{\alpha'_1}{u_1}^{x_1+\alpha' y_{11}+m' y_{21}}{u_2}^{x_2+\alpha' y_{12}+m' y_{22}} \equiv v \pmod p$$

outputting m' as the deciphered results (where $\alpha' = \alpha'_1 || \alpha'_2$), whereas if not satisfied, outputting as the decipher results the effect that the received ciphertext is rejected" as recited in independent claim 24.

iii. Independent Claim 28

One feature of the present invention, as recited in independent claim 28, includes a key generation step of generating a secret key and a public key. The secret key includes x_1, x_2, y_{11}, y_{12}, y_{21}, y_{22}, and z. The public key includes elements d_1 and d_2. The element d_1 relates to the elements y_{11} and y_{12} of the secret key, and the element d_2 relates to the elements y_{21} and y_{22} of the secret key. Cramer does not disclose this feature.

In response to Appellants' arguments that Cramer does not teach or suggest where the public key includes elements d_1 and d_2, the Examiner asserts on page 26 of the Examiner's Answer that Cramer teaches "d_i" (citing section V, column 9), and thus "d_i" can change and varies.

In response to the Examiner's arguments, Appellants note that in column 9, lines 57-58, Cramer discloses where the group element d is changed by $d_1, \ldots, d_k$, where $1 \leq i \leq k$. However, Cramer is silent as to the value of k used to implement the Cramer system. The present invention uses elements d_1 and d_2, which corresponds to k=2, and as previously discussed with reference to the Cramer Article, Appellants submit that in the actual implementation of Cramer, k is larger than or equal to 4.

In response to Appellants' arguments that Cramer does not teach or suggest where the secret key includes y_{11}, y_{12}, y_{21}, y_{22}, the Examiner asserts on page 28 of the Examiner's answer that Cramer expressly claims "choosing at least a first, second, and third . . ." (citing claim 1).

In response the Examiner's arguments, Appellants direct the Examiner's attention to the context and entirety of the language used in claim 1 of Cramer. The claim language of Cramer recites "choosing at least a first, second, and third exponent-number (x_1, x_2, z) as part of a private key." For example, as previously discussed, column 7, lines 11-19 of Cramer describes where a first exponent-number x_1, a second exponent-number x_2, a third exponent-number Z, a fourth exponent-number y_1, and a fifth exponent-number y_2, are chosen at random for the private key. As such, Cramer discloses the use of elements y_1 and y_2, and the "choosing at least a first, second, and third" language referred to in claim 1 of Cramer does not refer to "choosing at least a first, second, and third" of elements y_1 and y_2. Unlike Cramer, in the present invention, the secret key includes y_{11}, y_{12}, y_{21}, y_{22}. Cramer does not teach or suggest the additional elements of the claimed invention.

Furthermore, as previously discussed, Cramer teaches away from adding additional elements to obtain the present invention. As described in column 9, lines 65-67, Cramer describes where, in order to achieve security against lunch-time attacks, "one can simplify the above-described basic scheme" by omitting d, y_1 and y_2. As such, Cramer teaches away from adding additional elements, so as to include both elements d_1 and d_2 in the public key, and each of elements y_{11}, y_{12}, y_{21}, y_{22} in the secret key. Therefore,

contrary to the Examiner's assertions, it would not be obvious to modify Cramer to add the additional elements, so as to achieve the present invention.

In response to Appellants argument that Cramer teaches away from adding additional elements to obtain the present invention (i.e., y_{11}, y_{12}, y_{21}, y_{22}), the Examiner asserts on pages 28-29 that Cramer suggests the use of more elements (citing claims 1, 11 and 20). Specifically, the Examiner asserts that the language "choosing at least" implies that more elements may be added.

In response to the Examiner's arguments, Appellants direct the Examiner's attention to the specific language in claims 1, 11 and 20 that follows "choosing at least". There is no disclosure in claims 1, 11 or 20 of choosing at least elements including the element y. The "choosing at least" phrase precedes x_1, x_2, Z, g_1, g_2, etc., but does not precede the element y. Therefore, contrary to the Examiner's assertions, Cramer does teach away from adding the additional elements to obtain y_{11}, y_{12}, y_{21}, y_{22}, as in the present invention.

Therefore, Cramer fails to teach or suggest "a key generation step of generating a secret-key:

- $x_1, x_2, y_{11}, y_{12}, y_{21}, y_{22}, z \in \mathbb{Z}_q$

and a public-key:

- G, G' : finite (multiplicative) group $G \subseteq G'$
- q : prime number (the order of G)
- $g_1, g_2 \in G$
- $c = g_1^{x_1} g_2^{x_2}$, $d_1 = g_1^{y_{11}} g_2^{y_{12}}$, $d_2 = g_1^{y_{21}} g_2^{y_{22}}$, $h = g_1^{z}$,
- $\pi : X_1 \times X_2 \times M \longrightarrow G'$: one-to-one mapping
- $\pi^{-1} : \mathrm{Im}(\pi) \longrightarrow X_1 \times X_2 \times M$
- E : symmetric encipher function

where the group G is a partial group of the group G', X_1 and X_2 are an infinite set of positive integers which satisfy:

$$\alpha_1 || \alpha_2 < q \qquad (\forall \alpha_1 \in X_1, \forall \alpha_2 \in X_2)$$

where M is a key space" as recited in independent claim 28 of the present invention.

Another feature of the present invention, as recited in independent claim 28, includes a ciphertext generation and transmission step of selecting random numbers for key data K, calculating u_1, u_2, e, and v, where:

$$e = \pi(\alpha_1, \alpha_2, K)\, h_r \quad \text{, and} \quad v = g_1^{\alpha 1}\, c^r\, d_1^{\alpha r}\, d_2^{Kr} \quad .$$

Cramer does not disclose this feature.

In response to Appellants arguments that Cramer fails to teach or suggest $e = \pi(\alpha_1, \alpha_2, K)\, h_r$ and $v = g_1^{\alpha 1}\, c^r\, d_1^{\alpha r}\, d_2^{Kr}$, the Examiner asserts on page 27 of the Examiner's Answer (with reference to the rejection of claim 23) that Cramer expressly teaches performing calculations with the specific elements to obtain keys and decrypted data (citing claims 1 and 11; and column 11, lines 43-60). The Examiner further asserts that adding,

subtracting, raising to the power, or performing a mod operation without clearly defining what the numbers are do not patentably distinguish the present invention over the Cramer reference.

In response to the Examiner's arguments, Appellants submit that the elements contained in the claims are well known to one of ordinary skill in the art. Therefore, further defining the elements is not necessary. Furthermore, whether or not the terms are clearly defined, Cramer still fails to teach the features of the present invention, and is clearly different from the claimed invention.

For example, the verification cipher-number v, as calculated in Cramer (i.e., $v = c^r d^{ra}$) is quite different from v, as calculated in the present invention (i.e., $v = g_1^{a1} c^r d_1^{ar} d_2^{Kr}$), and the Examiner has not provided any explanation as to why one of ordinary skill in the art would be motivated to modify Cramer to obtain this feature. In the present invention, the calculation of v is improved and k can be a small number. This is quite different from Cramer, where as described in the Cramer Article, k is equal to or greater than 4. In the present invention, r can be set small, and the encryption calculation can be efficiently performed.

By way of further example, as shown in column 8, line 5, Cramer discloses where the encryption cipher-number e is calculated according to the following formula: $e = h^r m$. This is quite different from the present invention, where $e = \pi (\alpha_1, \alpha_2, K) h_n$, and the Examiner has not provided any explanation as to why one of ordinary skill in the art would be motivated to modify Cramer to obtain this feature.

In response to Appellants' arguments that the present invention distinguishes over Cramer because unlike Cramer, the present invention does not rely upon a hash function, and thus, does not use a hash-value a, as in Cramer, the Examiner asserts on page 25 of the Examiner's Answer that Cramer teaches that the use of a hash function can be omitted (citing column 9, lines 60-67).

In response to the Examiner's arguments, Appellants acknowledge that Cramer teaches where the hash function can be omitted. However, the present invention is different from Cramer in the feature used instead of the hash function. That is to say, the calculation of v is unique to the present invention. Specifically, the verification cipher-number v, as calculated in Cramer (i.e., $v = c^r d^a$) is quite different from v, as calculated in the present invention (i.e., $v = g_1^{\alpha 1} c^r d_1^{\alpha r} d_2^{Kr}$), and the Examiner has not provided any explanation as to why one of ordinary skill in the art would be motivated to modify Cramer to obtain this feature.

Therefore, Cramer fails to teach or suggest "a ciphertext generation and transmission step of selecting random numbers $\alpha_1 \in X_1$, $\alpha_2 \in X_2$, $r \in Zq$ for key data K ($K \in M$), calculating:

$$u_1 = g_1^r, \quad u_2 = g_2^r, \quad e = \pi(\alpha_1, \alpha_2, K)h^r, \quad v = g_1^{\alpha_1} c^r d_1^{\alpha r} d_2^{Kr}$$

where $\alpha = \alpha_1 || \alpha_2$, generating a ciphertext C of transmission data m by:

$$C = E_K(m)$$

by using a (symmetric cryptographic function E and key data K, and transmitting (u_1, u_2, e, v, C) as the ciphertext" as recited in independent claim 28.

Yet another feature of the present invention, as recited in independent claim 28, includes a ciphertext reception and decipher step. This step includes a condition, such that a step is performed of executing a decipher process, if the following is satisfied:

$$g_1^{\alpha'_1} u_1^{x_1+\alpha' y_{11}+K' y_{21}} u_2^{x_2+\alpha' y_{12}+K' y_{22}} = v$$

If the above condition is not satisfied, then a step is performed of outputting as the decipher results the effect that the received ciphertext is rejected. Cramer does not disclose this feature.

In response to Appellants arguments that Cramer fails to teach or suggest the above-identified condition, the Examiner asserts on page 27 of the Examiner's Answer (with regard to the rejection of claim 23) that Cramer expressly teaches performing calculations with the specific elements to obtain keys and decrypted data (citing claims 1 and 11; and column 11, lines 43-60). The Examiner further asserts that adding, subtracting, raising to the power, or performing a mod operation without clearly defining what the numbers are do not patentably distinguish the present invention over the Cramer reference.

In response to the Examiner's arguments, Appellants submit that the elements contained in the claims are well known to one of ordinary skill in the art. Therefore, further defining the elements is not necessary. Furthermore,

whether or not the terms are clearly defined, Cramer still fails to teach the features of the present invention, and is clearly different from the claimed invention.

For example, as described in column 8, lines 50-62, Cramer discloses a condition [1]: $u_1^{x1+y1a}\ u^{x2+y2a} = v$. The condition [1] of Cramer is not the same as the above-described condition of the present invention. Accordingly, Cramer does not disclose the claimed feature, and the Examiner has not provided any explanation as to why one of ordinary skill in the art would be motivated to modify Cramer to obtain this feature.

Therefore, Cramer fails to teach or suggest "a ciphertext reception and decipher step of calculating from the received ciphertext and by using the secret key, α'_1, α'_2, K' ($\alpha'_1 \epsilon X_1$, $\alpha'_2 \epsilon X_2$, $K' \epsilon M$) which satisfy:

$$\pi(\alpha'_1 || \alpha'_2 || K') = e/u_1^{z}$$

and if the following is satisfied:

$$g_1^{\alpha'_1} u_1^{x_1+\alpha' y_{11}+K' y_{21}} u_2^{x_2+\alpha' y_{12}+K' y_{22}} = v$$

where $\alpha' = \alpha'_1 || \alpha'_2$

executing a decipher process by:

$$m = D_{K'}(C)$$

outputting deciphered results, whereas if not satisfied, outputting as the decipher results the effect that the received ciphertext is rejected" as recited in independent claim 28.

iv. Independent Claim 30

One feature of the present invention, as recited in independent claim 30, includes a key generation step of generating a secret key and a public key. The secret key includes x_1, x_2, y_{11}, y_{12}, y_{21}, y_{22}, and z. The public key includes elements d_1 and d_2. The element d_1 relates to the elements y_{11} and y_{12} of the secret key, and the element d_2 relates to the elements y_{21} and y_{22} of the secret key. Cramer does not disclose this feature.

In response to Appellants' arguments that Cramer does not teach or suggest where the public key includes elements d_1 and d_2, the Examiner asserts on page 26 of the Examiner's Answer that Cramer teaches "d_i" (citing section V, column 9), and thus "d_i" can change and varies.

In response to the Examiner's arguments, Appellants note that in column 9, lines 57-58, Cramer discloses where the group element d is changed by $d_1, \ldots, d_k$, where $1 \leq i \leq k$. However, Cramer is silent as to the value of k used to implement the Cramer system. The present invention uses elements d_1 and d_2, which corresponds to k=2, and as previously discussed with reference to the Cramer Article, Appellants submit that in the actual implementation of Cramer, k is larger than or equal to 4.

In response to Appellants arguments that Cramer does not teach or suggest where the secret key includes y_{11}, y_{12}, y_{21}, y_{22}, the Examiner asserts that Cramer expressly claims "choosing at least a first, second, and third . . ." (citing claim 1).

In response the Examiner's arguments, Appellants direct the Examiner's attention to the context and entirety of the language used in claim 1 of Cramer. The claim language of Cramer recites "choosing at least a first, second, and third exponent-number (x_1, x_2, z) as part of a private key." As described in column 7, lines 11-19, Cramer discloses where a first exponent-number x_1, a second exponent-number x_2, a third exponent-number z, a fourth exponent-number y_1, and a fifth exponent-number y_2, are chosen at random for the private key. As such, Cramer discloses the use of elements y_1 and y_2, and the "choosing at least a first, second, and third" language referred to in claim 1 of Cramer does not refer to "choosing at least a first, second, and third" of elements y_1 and y_2. Unlike Cramer, in the present invention, the secret key includes y_{11}, y_{12}, y_{21}, y_{22}. Cramer does not teach or suggest the additional elements of the claimed invention, and the claim language of Cramer cited by the Examiner does not refer to the additional elements in the group y_{11}, y_{12}, y_{21}, y_{22} of the present invention.

Furthermore, as described in column 9, lines 65-67, Cramer describes where, in order to achieve security against lunch-time attacks, "one can simplify the above-described basic scheme" by omitting d, y_1 and y_2. As such, Cramer teaches away from adding additional elements, so as to include both elements d_1 and d_2 in the public key, and each of elements y_{11}, y_{12}, y_{21}, y_{22} in the secret key. Therefore, contrary to the Examiner's assertions, it would not be obvious to modify Cramer to add the additional elements, so as to achieve the present invention.

In response to Appellants argument that Cramer teaches away from adding additional elements to obtain the present invention (i.e., y_{11}, y_{12}, y_{21}, y_{22}), the Examiner asserts on pages 29-30 (with reference to the rejection of claim 30) that Cramer suggests the use of more elements (citing claims 1, 11 and 20). Specifically, the Examiner asserts that the language "choosing at least" implies that more elements may be added.

In response to the Examiner's arguments, Appellants direct the Examiner's attention to the specific language in claims 1, 11 and 20 that follows "choosing at least". There is no disclosure in claims 1, 11 or 20 of choosing at least elements including the element y. The "choosing at least" phrase precedes x_1, x_2, Z, g_1, g_2, etc., but does not precede the element y. Therefore, contrary to the Examiner's assertions, Cramer does teach away from adding the additional elements to obtain y_{11}, y_{12}, y_{21}, y_{22}, as in the present invention.

Therefore, Cramer fails to teach or suggest "a key generation step of generating a secret-key:

- $x_1, x_2, y_{11}, y_{12}, y_{21}, y_{22}, z \in \mathbb{Z}_q$

and a public-key:

- p, q : prime number (q is a prime factor of p-1)
- $g_1, g_2 \in \mathbb{Z}_p$: $\mathrm{ord}_p(g_1) = \mathrm{ord}_p(g_2) = q$
- $c = g_1^{x_1} g_2^{x_2} \bmod p$, $d_1 = g_1^{y_{11}} g_2^{y_{12}} \bmod p$, $d_2 = g_1^{y_{21}} g_2^{y_{22}} \bmod p$, $h = g_1^{z} \bmod p$,
- k_1, k_2, k_3 : positive constant $(10^{k_1+k_2} < q,\ 10^{k_3} < q,\ 10^{k_1+k_2+k_3} < p)$
- E : symmetric encipher function

" as recited in independent claim 30.

Another feature of the present invention, as recited in independent claim 30, includes a ciphertext generation and transmission step of selecting random numbers for key data K, calculating u_1, u_2, e, and v, where:

$$u_1 = g_1^r \bmod p, \quad u_2 = g_2^r \bmod p, \quad e = \tilde{m}\, h^r \bmod p, \quad v = g_1^{\alpha_1} c^r d_1^{\alpha r} d_2^{Kr} \bmod p$$

Cramer does not disclose this feature.

In response to Appellants' arguments that the present invention distinguishes over Cramer because unlike Cramer, the present invention does not rely upon a hash function, and thus, does not use a hash-value a, as in Cramer, the Examiner asserts on page 25 of the Examiner's Answer that Cramer teaches that the use of a hash function can be omitted (citing column 9, lines 60-67).

In response to the Examiner's arguments, Appellants acknowledge that Cramer teaches where the hash function can be omitted. However, the present invention is different from Cramer in the feature used instead of the hash function. The calculation of v is unique to the present invention.

For example, as described in column 7, line 56 to column 8, line 21, Cramer discloses where the encryption means computes a first universal cipher-number u_1, an encryption cipher-number e, a hash-value a, and a verification cipher-number v. The verification cipher-number v is based on the first group-number c, the third group-number d, the hash-value a, and the single exponent-number r. The present invention, as recited in claim 30, does

not rely upon a hash function, and thus, does not use a hash-value a. In this way, for example, Cramer is clearly different from the claimed invention. Specifically, the verification cipher-number v, as calculated in Cramer (i.e., $v = c^r d^a$) is quite different from v, as calculated in the present invention (i.e., $v = g_1^{a1} c^r d_1^{ar} d_2^{Kr} \bmod p$), and the Examiner has not provided any explanation as to why one of ordinary skill in the art would be motivated to modify Cramer to obtain this feature.

By way of further example, as shown in column 8, line 5, Cramer discloses the formulas used for calculating u_1, u_2, e, and v. As shown, Cramer does not disclose the use of modulo arithmetic in the equations used to calculate u_1, u_2, e, and v. This is quite different from the present invention, where the step of generating a public key includes where the elements u_1, u_2, e, and v are calculated using modulo arithmetic. Accordingly, Cramer does not teach generating a public key in the manner claimed, and the Examiner has not provided any explanation as to why one of ordinary skill in the art would be motivated to modify Cramer to obtain this feature.

In response to Appellants' arguments that Cramer does not teach or suggest the use of modulo arithmetic in the equations used to calculate u_1, u_2, e, and v, the Examiner does not provide any arguments for claim 30. However, as best can be determined, with reference to the Examiner's response regarding claim 23 on page 27 of the Examiner's Answer, it appears that the Examiner's position is that Cramer expressly teaches performing calculations with the specific elements to obtain keys and decrypted data (citing claims 1 and 11; and column 11, lines 43-60). Specifically, the

Examiner asserts that adding, subtracting, raising to the power, or performing a mod operation without clearly defining what the numbers are do not patentably distinguish the present invention over the Cramer reference.

In response to the Examiner's arguments, Appellants submit that the elements contained in the claims are well known to one of ordinary skill in the art. Therefore, further defining the elements is not necessary. Furthermore, whether or not the terms are clearly defined, Cramer still fails to teach the features of the present invention, and is clearly different from the claimed invention.

Therefore, Cramer fails to teach or suggest "a ciphertext generation and transmission step of selecting random numbers $a = a_1 || a_2$ ($|a_1| = k_1$, $|a_2| = k_2$) for key data K ($|K| = k_3$ where $|x|$ is the number of digits of x), calculating:

$$\tilde{m} = \alpha || K$$

selecting a random number $r \in Zq$, calculating:

$$u_1 = g_1^r \bmod p, \quad u_2 = g_2^r \bmod p, \quad e = \tilde{m} h^r \bmod p, \quad v = g_1^{\alpha_1} c^r d_1^{\alpha r} d_2^{Kr} \bmod p$$

and generating a ciphertext C of transmission data by:

$$C = E_K(m)$$

by using a (symmetric) cryptographic function E and the key data K, and transmitting (u_1, u_2, e, v, C) as the ciphertext" as recited in independent claim 30.

Yet another feature of the present invention, as recited in independent claim 30, includes a ciphertext reception and decipher step. This step includes a condition, such that a step is performed of executing a decipher process, if the following is satisfied:

$$g_1^{\alpha'_1} u_1^{x_1+\alpha' y_{11}+K' y_{21}} u_2^{x_2+\alpha' y_{12}+K' y_{22}} \equiv v \pmod{p}$$

If the above condition is not satisfied, then a step is performed of outputting, as the decipher results, the effect that the received ciphertext is rejected. Cramer does not disclose this feature.

In response to Appellants arguments that Cramer fails to teach or suggest the above-identified condition, the Examiner asserts on page 27 of the Examiner's Answer that Cramer expressly teaches performing calculations with the specific elements to obtain keys and decrypted data (citing claims 1 and 11; and column 11, lines 43-60). The Examiner further asserts that adding, subtracting, raising to the power, or performing a mod operation without clearly defining what the numbers are do not patentably distinguish the present invention over the Cramer reference.

In response to the Examiner's arguments, Appellants submit that the elements contained in the claims are well known to one of ordinary skill in the art. Therefore, further defining the elements is not necessary. Furthermore, whether or not the terms are clearly defined, Cramer still fails to teach the features of the present invention, and is clearly different from the claimed invention.

For example, as described in column 8, lines 50-62, Cramer discloses a condition [1]: $u_1^{x1+y1a}\, u^{x2+y2a} = v$. The condition [1] of Cramer is not the same as the above-described condition of the present invention. Accordingly, Cramer does not disclose the claimed feature, and the Examiner has not provided any explanation as to why one of ordinary skill in the art would be motivated to modify Cramer to obtain this feature.

Therefore, Cramer fails to teach or suggest "a ciphertext reception and decipher step of calculating from the received ciphertext and by using the secret key, α'_1, α'_2, K' ($|\alpha'_1| = k_1$, $|\alpha'_2| = k_2$, $|K'| = k_3$) which satisfy:

$$\alpha'_1 || \alpha'_2 || K' = e / u_1{}^z \bmod p$$

and if the following is satisfied:

$$g_1{}^{\alpha'_1} u_1{}^{x_1+\alpha' y_{11}+K' y_{21}} u_2{}^{x_2+\alpha' y_{12}+K' y_{22}} \equiv v \pmod p$$

where $\alpha' = \alpha'_1 || \alpha'_2$,

executing a decipher process by:

$$m = D_{K'}(C)$$

outputting deciphered results, whereas if not satisfied, outputting as the decipher results the effect that the received ciphertext is rejected" as recited in independent claim 30.

v. Independent Claim 35

One feature of the present invention, as recited in independent claim 35, includes a ciphertext generation and transmission step of selecting random numbers, calculating u_1, u_2, v, and K, where:

$$v = g_1^{a1}\, c^r\, d^{ar} \text{ , and } K = H(h^r) \text{ .}$$

Cramer does not disclose this feature.

In response to Appellants' arguments that the present invention distinguishes over Cramer because unlike Cramer, the present invention does not rely upon a hash function, and thus, does not use a hash-value a, as in Cramer, the Examiner asserts on page 30 of the Examiner's Answer that Cramer teaches that the use of a hash function can be omitted (citing column 9, lines 60-67).

In response to the Examiner's arguments, Appellants acknowledge that Cramer teaches where the hash function can be omitted. However, the present invention is different from Cramer in the feature used to calculate v. That is to say, the calculation of v is unique to the present invention. For example, unlike the present invention, Cramer does not rely upon g_1^{a1} in the calculation of v. In this way, for example, Cramer is clearly different from the claimed invention. Specifically, the verification cipher-number v, as calculated in Cramer (i.e., $v = c^r\, d^{r\alpha}$) is quite different from v, as calculated in the present invention (i.e., $v = g_1^{a1}\, c^r\, d^{ar}$), and the Examiner has not provided any explanation as to why one of ordinary skill in the art would be motivated to modify Cramer to obtain this feature.

In response to the Examiner's arguments that as loosely defined, K can be interpreted as a hash value, Applicants submit that the calculation of K is not the same as the calculation of v. Specifically, the verification cipher-number v, as calculated in Cramer (i.e., $v = c^r d^{r_0}$) is quite different from v, as calculated in the present invention (i.e., $v = g_1^{\alpha_1} c^r d^{\alpha r}$). Cramer uses a hash value in its calculation, and the present invention does not use such value in its calculation of v. The present invention distinguishes over Cramer in what is used instead of the hash value in its calculation of v. Therefore, the present invention is not the same as Cramer.

Therefore, Cramer fails to teach or suggest "a ciphertext generation and transmission step of selecting random numbers $\alpha_1 \in X_1$, $\alpha_2 \in X_2$, $r \in Z_q$, calculating:

$$u_1 = g_1^r, \quad u_2 = g_2^r, \quad v = g_1^{\alpha_1} c^r d^{\alpha r}, \quad K = H(h^r)$$

where $\alpha = \alpha_1 \| \alpha_2$, generating a ciphertext C of transmission data m by

$$C = E_K(\pi(\alpha_1, \alpha_2, m))$$

by using a (symmetric) cryptographic function E; and transmitting (u_1, u_2, v, C) as the ciphertext" as recited in independent claim 35.

Another feature of the present invention, as recited in independent claim 35, includes a ciphertext reception and decipher step. This step includes a condition, such that a step of outputting m' as the deciphered results if the following is satisfied:

$$g_1{}^{\alpha'_1} u_1{}^{x_1+\alpha' y_1} u_2{}^{x_2+\alpha' y_2} = v,$$

If the above condition is not satisfied, then a step of outputting as the decipher results the effect that the received ciphertext is rejected. Cramer does not disclose this feature. To support the assertion that Cramer teaches this feature, the Examiner cites columns 9-11. However, neither the cited text nor any other portions of Cramer, teach or suggest the claimed features.

In response to Appellants' arguments that Cramer fails to teach or suggest the above-identified condition, the Examiner asserts on page 27 of the Examiner's Answer (with reference to the rejection of claim 23) that Cramer expressly teaches performing calculations with the specific elements to obtain keys and decrypted data (citing claims 1 and 11; and column 11, lines 43-60). The Examiner further asserts that adding, subtracting, raising to the power, or performing a mod operation without clearly defining what the numbers are do not patentably distinguish the present invention over the Cramer reference.

In response to the Examiner's arguments, Appellants submit that the elements contained in the claims are well known to one of ordinary skill in the art. Therefore, further defining the elements is not necessary. Furthermore, whether or not the terms are clearly defined, Cramer still fails to teach the features of the present invention, and is clearly different from the claimed invention.

For example, as described in column 8, lines 50-62, Cramer discloses a condition [1]: $u_1^{x1+y1a}\ u^{x2+y2a} = v$. The condition [1] of Cramer is not the same as the above-described condition of the present invention. Accordingly, Cramer does not disclose the claimed feature, and the Examiner has not provided any explanation as to why one of ordinary skill in the art would be motivated to modify Cramer to obtain this feature.

Therefore, Cramer fails to teach or suggest "a ciphertext reception and decipher step of calculating:

$$K' = H(u_1^{z})$$

by using the secret key, calculating from the received ciphertext, α'_1, α'_2 (where $\alpha'_1 \in X_1$ $\alpha'_2 \in X_2$) which satisfy:

$$\pi(\alpha'_1, \alpha'_2, m') = D_{K'}(C)$$

if the following is satisfied:

$$g_1^{\alpha'_1} u_1^{x_1+\alpha' y_1} u_2^{x_2+\alpha' y_2} = v,$$

where $\alpha' = \alpha'_1 \| \alpha'_2$

outputting m' as the deciphered results, whereas if not satisfied, outputting as the decipher results the effect that the received ciphertext is rejected" as recited in independent claim 35.

vi. Independent Claim 36

On page 31 of the Examiner's Answer, the Examiner provides a

response to an argument that the present invention "uses 2 more elements than Cramer". In response to the Examiner, Appellants respectfully submit that this argument was not made with regard to claim 36.

One feature of the present invention, as recited in independent claim 36, includes a ciphertext generation and transmission step of selecting random numbers, calculating u_1, u_2, v, and K, where:

$$u_1 = g_1^r \bmod p, \quad u_2 = g_2^r \bmod p, \quad v = g_1^{\alpha_1} c^r d^{\alpha r} \bmod p, \quad K = H(h^r \bmod p)$$

Cramer does not disclose this feature.

In response to Appellants' arguments that the present invention distinguishes over Cramer because unlike Cramer, the present invention does not rely upon a hash function, and thus, does not use a hash-value a, as in Cramer, the Examiner asserts on page 25 of the Examiner's Answer that Cramer teaches that the use of a hash function can be omitted (citing column 9, lines 60-67).

In response to the Examiner's arguments, Appellants acknowledge that Cramer teaches where the hash function can be omitted. However, the present invention is different from Cramer in the feature used instead of the hash function. That is to say, the calculation of v is unique to the present invention. Specifically, the verification cipher-number v, as calculated in Cramer (i.e., $v = c^r d^{ra}$) is quite different from v, as calculated in the present invention (i.e., $v = g_1^{\alpha 1} c^r d^{\alpha r} \bmod p$), and the Examiner has not provided any

explanation as to why one of ordinary skill in the art would be motivated to modify Cramer to obtain this feature.

In response to Appellants' arguments that Cramer does not teach or suggest the use of modulo arithmetic in the equations used to calculate u_1, u_2, v, and K, the Examiner asserts on page 31 of the Examiner's Answer that Cramer expressly teaches performing calculations with the specific elements to obtain keys and decrypted data (citing claims 1 and 11; and column 11, lines 43-60). Specifically, the Examiner asserts that adding, subtracting, raising to the power, or performing a mod operation without clearly defining what the numbers are do not patentably distinguish the present invention over the Cramer reference.

In response to the Examiner's arguments, Appellants submit that the elements contained in the claims are well known to one of ordinary skill in the art. Therefore, further defining the elements is not necessary. Furthermore, whether or not the terms are clearly defined, Cramer still fails to teach the features of the present invention, and is clearly different from the claimed invention.

For example, as shown in column 8, line 5, Cramer discloses the formulas used for calculating u_1, u_2, e, and v. As shown, Cramer does not disclose the use of modulo arithmetic in the equations used to calculate u_1, u_2, e, v. This is quite different from the present invention, where the step of generating a public key includes where the elements u_1, u_2, v, and K are calculated using modulo arithmetic. Accordingly, Cramer does not teach generating a public key in the manner claimed, and the Examiner has not

provided any explanation as to why one of ordinary skill in the art would be motivated to modify Cramer to obtain this feature.

Therefore, Cramer fails to teach or suggest "a ciphertext generation and transmission step of selecting random numbers $\alpha = \alpha_1 || \alpha_2$ ($|\alpha_1| = k_1$, $|\alpha_2| = k_2$, where ($|x|$ is the number of digits of x), selecting a random number $r \in Zq$, calculating:

$$u_1 = g_1^r \bmod p, \quad u_2 = g_2^r \bmod p, \quad v = g_1^{\alpha_1} c^r d^{\alpha r} \bmod p, \quad K = H(h^r \bmod p)$$

transmitting the ciphertext (u_1, u_2, v, C); generating a ciphertext C of transmission data m by:

$$C = E_K(\alpha_1 || \alpha_2 || m)$$

by using a (symmetric) cryptographic function, and transmitting (u_1, u_2, v, C) as the ciphertext" as recited in independent claim 36.

Another feature of the present invention, as recited in independent claim 36, includes a ciphertext reception and decipher step. This step includes a condition, such that a step of outputting m' as the deciphered results if the following is satisfied:

$$g_1^{\alpha'_1} u_1^{x_1 + \alpha' y_1} u_2^{x_2 + \alpha' y_2} \equiv v \pmod p$$

If the above condition is not satisfied, then a step of outputting as the decipher results the effect that the received ciphertext is rejected. Cramer does not disclose this feature. To support the assertion that Cramer teaches this

feature, the Examiner cites columns 9-11. However, neither the cited text nor any other portions of Cramer teach or suggest the claimed features.

In response to Appellants' arguments that Cramer fails to teach or suggest the above-identified condition, the Examiner asserts on page 27 of the Examiner's Answer that Cramer expressly teaches performing calculations with the specific elements to obtain keys and decrypted data (citing claims 1 and 11; and column 11, lines 43-60). The Examiner further asserts that adding, subtracting, raising to the power, or performing a mod operation without clearly defining what the numbers are do not patentably distinguish the present invention over the Cramer reference.

In response to the Examiner's arguments, Appellants submit that the elements contained in the claims are well known to one of ordinary skill in the art. Therefore, further defining the elements is not necessary. Furthermore, whether or not the terms are clearly defined, Cramer still fails to teach the features of the present invention, and is clearly different from the claimed invention.

For example, as described in column 8, lines 50-62, Cramer discloses a condition [1]: $u_1^{x1+y1a}\ u^{x2+y2a} = v$. The condition [1] of Cramer is not the same as the above-described condition of the present invention. Accordingly, Cramer does not disclose the claimed feature, and the Examiner has not provided any explanation as to why one of ordinary skill in the art would be motivated to modify Cramer to obtain this feature.

Therefore, Cramer fails to teach or suggest "a ciphertext reception and decipher step of calculating:

$$K' = H(u_1{}^z \bmod p)$$

by using the secret key, calculating from the received ciphertext, α'_1, α'_2 ($|\alpha'_1| = k_1$, $|\alpha'_2| = k_2$) which satisfy:

$$\alpha'_1 || \alpha'_2 || m' = D_{K'}(C)$$

and if the following is satisfied:

$$g_1{}^{\alpha'_1} u_1{}^{x_1+\alpha' y_1} u_2{}^{x_2+\alpha' y_2} \equiv v \pmod p$$

outputting m' as the deciphered results (where $\alpha' = \alpha'_1 || \alpha'_2$), whereas if not satisfied, outputting as the decipher results the effect that the received ciphertext is rejected" as recited in independent claim 36.

vii. Independent Claim 40

One feature of the present invention, as recited in independent claim 40, includes a ciphertext generation and transmission step of selecting random numbers, calculating u_1, u_2 and v, where:

$$v = g_1{}^{a1}\, c^r\, d^{ar} \quad .$$

Cramer does not disclose this feature.

On page 32 of the Examiner's Answer, the Examiner provides a response to an argument that the present invention "Cramer does not expressly teach 'transmitting u_1, u_2, e, and v'". In response to the Examiner, Appellants respectfully submit that this argument was not made with regard to

claim 40. To the contrary, Appellants argued that the calculation of v, in the present invention, is different from the calculation of v, as in Cramer.

In response to Appellants' arguments that the present invention distinguishes over Cramer because unlike Cramer, the present invention does not rely upon a hash function in the calculation of v, and thus, does not use a hash-value a, as in Cramer, the Examiner asserts on page 25 of the Examiner's Answer that Cramer teaches that the use of a hash function can be omitted (citing column 9, lines 60-67).

In response to the Examiner's arguments, Appellants acknowledge that Cramer teaches where the hash function can be omitted. However, the present invention is different from Cramer in the feature used instead of the hash function. That is to say, the calculation of v is unique to the present invention. Specifically, the verification cipher-number v, as calculated in Cramer (i.e., $v = c^r d^{ra}$) is quite different from v, as calculated in the present invention (i.e., $v = g_1^{\alpha 1} c^r d^{\alpha r}$), and the Examiner has not provided any explanation as to why one of ordinary skill in the art would be motivated to modify Cramer to obtain this feature.

Therefore, Cramer fails to teach or suggest " a ciphertext generation and transmission step of selecting random numbers $\alpha_1 \in X_1$, $\alpha_2 \in X_2$, $r \in Zq$, calculating:

$$u_1 = g_1^r, \quad u_2 = g_2^r, \quad v = g_1^{\alpha_1} c^r d^{\alpha r}$$

where $\alpha = \alpha_1 \| \alpha_2$, generating a ciphertext C of transmission data m by:

$$e = E_{pk}(\pi(\alpha_1, \alpha_2, m))$$

by using an (asymmetric) cryptographic function E_{pk}, and transmitting (u_1, u_2, e, v) as the ciphertext" as recited in independent claim 40.

Another feature of the present invention, as recited in independent claim 40, includes a ciphertext reception and decipher step. This step includes a condition, such that a step of outputting m' as the deciphered results if the following is satisfied:

$$g_1^{\alpha'_1} u_1^{x_1+\alpha' y_1} u_2^{x_2+\alpha' y_2} = v,$$

If the above condition is not satisfied, then a step of outputting as the decipher results the effect that the received ciphertext is rejected. Cramer does not disclose this feature.

In response to Appellants' arguments that Cramer fails to teach or suggest the above-identified condition, the Examiner asserts on page 27 of the Examiner's Answer (with regard to the rejection of claim 23) that Cramer expressly teaches performing calculations with the specific elements to obtain keys and decrypted data (citing claims 1 and 11; and column 11, lines 43-60). The Examiner further asserts that adding, subtracting, raising to the power, or performing a mod operation without clearly defining what the numbers are do not patentably distinguish the present invention over the Cramer reference.

In response to the Examiner's arguments, Appellants submit that the elements contained in the claims are well known to one of ordinary skill in the art. Therefore, further defining the elements is not necessary. Furthermore, whether or not the terms are clearly defined, Cramer still fails to teach the features of the present invention, and is clearly different from the claimed invention.

For example, as described in column 8, lines 50-62, Cramer discloses a condition [1]: $u_1^{x1+y1a}\ u^{x2+y2a} = v$. The condition [1] of Cramer is not the same as the above-described condition of the present invention. Accordingly, Cramer does not disclose the claimed feature, and the Examiner has not provided any explanation as to why one of ordinary skill in the art would be motivated to modify Cramer to obtain this feature.

Therefore, Cramer fails to teach or suggest "a ciphertext reception and decipher step of calculating from the received ciphertext and by using the secret key, α'_1, α'_2, m' ($\alpha'_1 \in X_1$, $\alpha'_2 \in X_2$, $m' \in M$) which satisfy:

$$\pi(\alpha'_1, \alpha'_2, m') = D_{sk}(e)$$

and if the following is satisfied:

$$g_1^{\alpha'_1} u_1^{x_1+\alpha' y_1} u_2^{x_2+\alpha' y_2} = v$$

where:

$$\alpha' = \alpha'_1 || \alpha'_2$$

outputting m' as the deciphered results, whereas if not satisfied, outputting as the decipher results the effect that the received ciphertext is rejected" as recited in independent claim 40.

vii. Independent Claim 41

On page 41 of the Examiner's Answer, the Examiner provides a response to an argument that the present invention "uses 2 more elements than Cramer". In response to the Examiner, Appellants respectfully submit that this argument was not made with regard to claim 41.

One feature of the present invention, as recited in independent claim 41, includes a ciphertext generation and transmission step of selecting random numbers, calculating u_1, u_2 and v, where:

$$u_1 = g_1^{r} \bmod p, \quad u_2 = g_2^{r} \bmod p, \quad v = g_1^{\alpha_1} c^{r} d^{\alpha r} \bmod p$$

Cramer does not disclose this feature.

In response to Appellants' arguments that the present invention distinguishes over Cramer because unlike Cramer, the present invention does not rely upon a hash function, and thus, does not use a hash-value a, as in Cramer, the Examiner asserts on page 25 of the Examiner's Answer that Cramer teaches that the use of a hash function can be omitted (citing column 9, lines 60-67).

In response to the Examiner's arguments, Appellants acknowledge that Cramer teaches where the hash function can be omitted. However, the

present invention is different from Cramer in the feature used instead of the hash function. That is to say, the calculation of v is unique to the present invention. Specifically, the verification cipher-number v, as calculated in Cramer (i.e., $v = c^r d^{[a]}$) is quite different from v, as calculated in the present invention (i.e., $v = g_1^{a1} c^r d^{ar} \bmod p$), and the Examiner has not provided any explanation as to why one of ordinary skill in the art would be motivated to modify Cramer to obtain this feature.

In response to Appellants' arguments that Cramer does not teach or suggest the use of modulo arithmetic in the calculation of u_1, u_2 and v, the Examiner asserts that Cramer provides the teachings of using modulo arithmetic to generate the verification value (citing column 7, lines 60-67 and column 8, lines 1-10).

In response to the Examiner's arguments, Appellants submit that column 7, lines 60-67 to column 8, lines 1-10 refer to the modulo of element q. Specifically, Cramer discloses where a single exponent-number r is chose at random in an r-choosing step from a set of elements modulo q, denoted as Z_q. This use of modulo arithmetic in Cramer is not the same as the use of modulo arithmetic in the calculation of u_1, u_2 and v, in the manner claimed.

For example, as shown in column 8, line 5, Cramer discloses the formulas used for calculating u_1, u_2 and v. As shown, Cramer does not disclose the use of modulo arithmetic in the equations used to calculate u_1, u_2 and v. This is quite different from the present invention, where the step of generating a public key includes where the elements u_1, u_2 and v, are calculated using modulo arithmetic. Accordingly, Cramer does not teach

generating a public key in the manner claimed, and the Examiner has not provided any explanation as to why one of ordinary skill in the art would be motivated to modify Cramer to obtain this feature.

Therefore, Cramer fails to teach or suggest "a ciphertext generation and transmission step of selecting random numbers $\alpha = \alpha_1 || \alpha_2$ ($|\alpha_1| = k_1$, $|\alpha_2| = k_2$, where $|x|$ is the number of digits of x), selecting a random number $r \in Zq$, calculating:

$$u_1 = g_1^r \bmod p, \quad u_2 = g_2^r \bmod p, \quad v = g_1^{\alpha_1} c^r d^{\alpha r} \bmod p$$

generating a ciphertext C of transmission data m (positive integer) by:

$$e = E_{pk}(\alpha_1 || \alpha_2 || m)$$

by using the secret key, and transmitting (u_1, u_2, e, v) as the ciphertext" as recited in independent claim 41.

Another feature of the present invention, as recited in independent claim 41, includes a ciphertext reception and decipher step. This step includes a condition, such that a step of outputting m' as the deciphered results if the following is satisfied:

$$g_1^{\alpha'_1} u_1^{x_1 + \alpha' y_1} u_2^{x_2 + \alpha' y_2} \equiv v \pmod p$$

If the above condition is not satisfied, then a step of outputting as the decipher results the effect that the received ciphertext is rejected. Cramer does not disclose this feature.

In response to Appellants' arguments that Cramer fails to teach or suggest the above-identified condition, the Examiner asserts on page 27 of the Examiner's Answer (with regard to the rejection of claim 23) that Cramer expressly teaches performing calculations with the specific elements to obtain keys and decrypted data (citing claims 1 and 11; and column 11, lines 43-60). The Examiner further asserts that adding, subtracting, raising to the power, or performing a mod operation without clearly defining what the numbers are do not patentably distinguish the present invention over the Cramer reference.

In response to the Examiner's arguments, Appellants submit that the elements contained in the claims are well known to one of ordinary skill in the art. Therefore, further defining the elements is not necessary. Furthermore, whether or not the terms are clearly defined, Cramer still fails to teach the features of the present invention, and is clearly different from the claimed invention.

For example, as described in column 8, lines 50-62, Cramer discloses a condition [1]: $u_1^{x1+y1a}\, u^{x2+y2a} = v$. The condition [1] of Cramer is not the same as the above-described condition of the present invention. Accordingly, Cramer does not disclose the claimed feature, and the Examiner has not provided any explanation as to why one of ordinary skill in the art would be motivated to modify Cramer to obtain this feature.

Therefore, Cramer fails to teach or suggest "a ciphertext reception and decipher step of calculating from the received ciphertext and by using the secret key, α'_1, α'_2, m' ($|\alpha'_1| = k_1$, $|\alpha'_2| = k_2$, m' is a positive integer) which satisfy:

$$\alpha_1' || \alpha_2' || m' = D_{sk}(e)$$

and if the following is satisfied:

$$g_1^{\alpha_1'} u_1^{x_1 + \alpha' y_1} u_2^{x_2 + \alpha' y_2} \equiv v \pmod{p},$$

where:

$$\alpha' = \alpha_1' || \alpha_2'$$

outputting m' as the deciphered results, whereas if not satisfied, outputting as the decipher results the effect that the received ciphertext is rejected" as recited in independent claim 41.

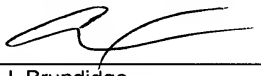
C. Conclusion

Therefore, based on the above remarks, Appellants submit that the Examiner's final rejection of claims 23-44 under 35 USC §112, second paragraph; and the rejection of claims 23-44 USC §103(a) are not properly founded in law and respectfully request that the Board of Patent Appeal Interferences reverse the Examiner's final rejection.

To the extent necessary, Appellants petition for an extension of time under 37 CFR §1.136. Please charge any shortage in the fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account No. 50-1417 (Case No. 500.41092X00) and please credit any excess fees to such Deposit Account.

Respectfully submitted,

MATTINGLY, STANGER, MALUR & BRUNDIDGE, P.C.



Carl I. Brundidge
Registration No. 29,621

CIB/DKM/cmd
(703) 684-1120
Enclosures

VIII. CLAIMS APPENDIX

The copy of the claims contained in the Appendix to the Appeal Brief is correct, as the Examiner affirmed in the Examiner's Answer.

IX. EVIDENCE APPENDIX

The statement of the evidence contained in the Appeal Brief is correct, as the Examiner affirmed in the Examiner's answer.

Accordingly, there is no evidence relied upon in this Appeal.

X. RELATED PROCEEDINGS APPENDIX

The statement of the related proceedings contained in the Appeal Brief is correct, as the Examiner affirmed in the Examiner's Answer.

Accordingly, there are no related proceedings.

XI. FEES

To the extent necessary, Appellants petition for an extension of time under 37 CFR §1.136. Please charge any shortage in the fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account No. 50-1417 (Case No. 500.41092X00) and please credit any excess fees to such Deposit Account.

Respectfully submitted,

MATTINGLY, STANGER, MALUR & BRUNDIDGE, P.C.

Carl I. Brundidge
Registration No. 29,621

CIB/DKM/cmd
(703) 684-1120
Enclosures (in triplicate)